Weight Distributions of Regular Low-Density Parity-Check Codes over Finite Fields

Shengtian Yang, *Member, IEEE,* Thomas Honold, *Member, IEEE,* Yan Chen, *Member, IEEE,*
Zhaoyang Zhang, *Member, IEEE,* Peiliang Qiu, *Member, IEEE*

***Abstract*—The average weight distribution of a regular low-density parity-check (LDPC) code ensemble over a finite field is thoroughly analyzed. In particular, a precise asymptotic approximation of the average weight distribution is derived for the small-weight case, and a series of fundamental qualitative properties of the asymptotic growth rate of the average weight distribution are proved. Based on this analysis, a general result, including all previous results as special cases, is established for the minimum distance of individual codes in a regular LDPC code ensemble.**

***Index Terms*—Low-density parity-check (LDPC) codes, minimum distance, weight distribution.**

I. Introduction

LOW-DENSITY parity-check (LDPC) codes, originally introduced by Gallager [1], are a family of linear codes characterized by a sparse parity-check matrix. Owing to their capacity-approaching performance under low-complexity iterative decoding algorithms, LDPC codes have attracted tremendous attention in the past years. To evaluate the theoretical performance of an LDPC code, a typical method is to estimate its performance under maximum-likelihood (ML) or iterative decoding assumptions. The performance of a linear code under ML decoding can be well estimated based on its weight distribution [1], so having the knowledge about weight distributions of LDPC codes facilitate the analysis of the ML decoding performance.

The first analysis work on the weight distributions of LDPC codes was given by Gallager in his pioneering work [1], where he studied the weight distributions of binary regular LDPC codes. Moreover, he also generalized the analysis to non-binary regular LDPC codes over $\mathbb{Z}_m$ ($m > 2$), characterized by zero-one parity-check matrices. Ever since the publication of [1], there has been a lot of work extending the analysis of weight distributions of binary LDPC codes in different ways, such as [2]–[7]. A generalization of weight distributions, also known as spectra, of regular LDPC codes over finite fields and arbitrary abelian groups were later studied in [8], [9]. More recently, the binary weight distributions of non-binary LDPC codes also received some attention [10]. By now a bundle of formulas about weight distributions of various LDPC codes is known, but the value and significance of most formulas is far from being fully understood, except in the case of binary regular LDPC codes, which have been well studied [1], [2]. The difficulty is due to the complex expressions for the weight distributions of LDPC codes, which are usually obtained by the generating function approach and hence are typically expressed as coefficients of a polynomial. Given a polynomial $p(x)$ with nonnegative coefficients, a usual approach for estimating the coefficient of a monomial x^k in $[p(x)]^n$ is to calculate the infimum of $[p(x)]^n/x^k$ over all positive x, which gives an upper bound of the coefficient and in fact has the same asymptotic growth rate as the coefficient [4, Theorem 1]. However, analyzing functions like $\inf_{y>0} f(x, y)$ is not an easy job. When $f(x, y)$ is complicated, determining the shape, such as monotonicity, convexity, and zeros, of $\inf_{y>0} f(x, y)$ becomes a difficult mission.

In this paper, we shall perform such a mission for ensembles of regular LDPC codes over finite fields. At first, as an easy consequence of the results in [8], [9], [11], an exact expression is introduced for the average weight distribution of a (c, d)-regular LDPC code ensemble over the finite field $\mathbb{F}_q$ of order q, where c and d, in a less strict sense, correspond to the column and row weight of parity-check matrix, respectively. Based on this expression, we show that, when averaged on the whole ensemble, the fraction of codewords of small weight l in an LDPC code is at most asymptotically $n^{-\lceil (c-2)l/2 \rceil}$ as the coding length n goes to infinity. Next, using the upper-bound technique mentioned above, we analyze the asymptotic growth rate $\omega_{q,c,d}(x)$ of the average weight distribution, where x denotes the normalized weight. A series of fundamental qualitative properties of $\omega_{q,c,d}(x)$ are found and proved. In particular, we show that for $d \ge c \ge 3$, $\omega_{q,c,d}(x)$ has a unique zero x_0 in $(0, 1 - 1/q]$. This zero just corresponds to the normalized minimum distance of a typical LDPC code, and hence provides important information about the code ensemble. Finally, we prove that for $d \ge c \ge 3$, there are at most a fraction $\Theta(n^{-\lceil (c-2)l_0/2 \rceil})$ of all codes in the ensemble whose minimum distance is between the constant l_0 and αn,

This work was supported in part by the National Natural Science Foundation of China under Grants 60772093, 60802014, and 60872063, the Chinese Specialized Research Fund for the Doctoral Program of Higher Education under Grants 200803351023 and 200803351027, the National High Technology Research and Development Program of China under Grant 2007AA01Z257, the Zhejiang Provincial Natural Science Foundation of China under Grant Y106068, and the Program for New Century Excellent Talents in University under grant NCET-09-0701.

S. Yang is self-employed at Zhengyuan Xiaoqu 10-2-101, Hangzhou 310011, China (email: yangst@codlab.net).

T. Honold is with the Department of Information Science and Electronic Engineering, Zhejiang University, Hangzhou 310027, China (email: honold@zju.edu.cn).

Y. Chen is with Huawei Technologies Co., Ltd (Shanghai), Shanghai 201206, China (email: eeyanchen@huawei.com).

Z. Zhang and P. Qiu are with the Department of Information Science and Electronic Engineering, Zhejiang University, Hangzhou 310027, China (email: ning_ming@zju.edu.cn; qiupl@zju.edu.cn).

where $\alpha \in (0, x_0)$.

The rest of this paper is organized as follows. In Section II, we introduce the notations and conventions to be used throughout the paper. In Section III, we define the ensemble of regular LDPC codes over a finite field and give its average weight distribution function; moreover, we study the asymptotic behavior of the average weight distribution for the small-weight case. The main analysis, consisting of two stages, for the asymptotic growth rate of the average weight distribution is performed in Sections IV and V. The minimum distance of individual codes in a regular LDPC code ensemble is analyzed in Section VI. Section VII concludes the paper.

II. Notations and Conventions

In this section, we introduce some basic notations and conventions to be used throughout the rest of this paper.

- In general, symbols, real variables, and deterministic mappings are denoted by lowercase letters. Sets and random elements are denoted by capital letters.
- The symbols $\mathbb{Z}$, $\mathbb{N}$, $\mathbb{N}_0$, $\mathbb{R}$ denote the ring of integers, the set of positive integers, the set of nonnegative integers, and the field of real numbers, respectively. For a prime power $q \geq 2$ the finite field of order q is denoted by $\mathbb{F}_q$. The multiplicative subgroup of nonzero elements of $\mathbb{F}_q$ is denoted by $\mathbb{F}_q^\times$.
- The n-fold cartesian product of a set A is denoted by A^n. An element of A^n is denoted by $\mathbf{x} = (x_1, x_2, \ldots, x_n)$, where $x_i \in A$ denotes the ith component of $\mathbf{x}$.
- For any vector $\mathbf{c} \in \mathbb{F}_q^n$, the *weight* $w(\mathbf{c})$ of $\mathbf{c}$ is the number of nonzero symbols in it, that is, $w(\mathbf{c}) \triangleq |\{i : c_i \neq 0\}|$.
- Given the functions $f : X \to Y$ and $g : Y \to Z$, their composite is the function $g \circ f : X \to Z$ given by $x \mapsto g(f(x))$.
- Given the functions $f : X_1 \to Y_1$ and $g : X_2 \to Y_2$, their cartesian product is the function $f \odot g : X_1 \times X_2 \to Y_1 \times Y_2$ given by $(x_1, x_2) \mapsto (f(x_1), g(x_2))$.
- When performing probabilistic analysis, all objects of study are relative to a basic probability space $(\Omega, \mathcal{A}, P)$ where $\mathcal{A}$ is a σ-algebra in Ω and P is a probability measure on $(\Omega, \mathcal{A})$. For any event $A \in \mathcal{A}$, $PA = P(A)$ is called the probability of A. Any measurable mapping of Ω into some measurable space $(B, \mathcal{B})$ is generally called a random element. For any random set or function, we tacitly assume that their n-fold cartesian products (e.g., A^n or $\bigodot_{i=1}^n F$) are cartesian products of their independent copies.
- All logarithms are taken to the natural base e and denoted by $\ln$.
- For any $x \in [0, 1]$ and any integer $q \geq 2$, the *entropy function* $H_q(x)$ is defined by
$$H_q(x) \triangleq x \ln \frac{1}{x} + (1 - x) \ln \frac{1}{1 - x} + x \ln(q - 1).$$
For any $x, y \in [0, 1]$, the *information divergence function* $D(x\|y)$ is defined by
$$D(x\|y) \triangleq x \ln \frac{x}{y} + (1 - x) \ln \frac{1 - x}{1 - y}.$$
- For any real functions $f(n)$ and $g(n)$ with $n \in \mathbb{N}$, the asymptotic Θ-notation $f(n) = \Theta(g(n))$ means that there exist positive constants c_1 and c_2 such that
$$c_1 g(n) \leq f(n) \leq c_2 g(n).$$
for sufficiently large n.
- For $x \in \mathbb{R}$, $\lfloor x \rfloor$ denotes the largest integer not exceeding x, and $\lceil x \rceil$ denotes the smallest integer not less than x.

III. Regular LDPC Codes over Finite Fields

We first define some basic $\mathbb{F}_q$-linear transformations.

Definition 3.1: A *single symbol repetition* with a parameter $c \in \mathbb{N}$ is a mapping $f_{q,c}^{\mathrm{REP}} : \mathbb{F}_q \to \mathbb{F}_q^c$ given by $x \mapsto (x, x, \ldots, x)$.

Definition 3.2: A *single symbol check* with a parameter $d \in \mathbb{N}$ is a mapping $f_{q,d}^{\mathrm{CHK}} : \mathbb{F}_q^d \to \mathbb{F}_q$ given by $\mathbf{x} \mapsto \sum_{i=1}^d x_i$.

Definition 3.3: A *single symbol random multiplier map* is a random mapping $F_q^{\mathrm{RM}} : \mathbb{F}_q \to \mathbb{F}_q$ given by $x \to Cx$ where C is an independent random variable uniformly distributed over $\mathbb{F}_q^\times$.

Definition 3.4: A *uniform random interleaver* of $\mathbb{F}_q^n$ is a random automorphism $\Sigma_{q,n} : \mathbb{F}_q^n \to \mathbb{F}_q^n$ given by $\mathbf{x} \mapsto (x_{\Pi^{-1}(1)}, x_{\Pi^{-1}(2)}, \ldots, x_{\Pi^{-1}(n)})$, where Π is an independent random permutation uniformly distributed over the symmetric group S_n, i.e., all permutations on n letters.

Next, we define a random linear transformation based on the above simple maps.

Definition 3.5: $F_{q,c,d,n}^{\mathrm{LD}} : \mathbb{F}_q^n \to \mathbb{F}_q^{cn/d}$ is a random mapping defined by
$$F_{q,c,d,n}^{\mathrm{LD}} \triangleq f_{q,d,cn/d}^{\mathrm{CHK}} \circ F_{q,cn}^{\mathrm{RM}} \circ \Sigma_{q,cn} \circ f_{q,c,n}^{\mathrm{REP}} \tag{1}$$
where $c, d \in \mathbb{N}$, d divides cn, and
$$f_{q,c,n}^{\mathrm{REP}} \triangleq \bigodot_{i=1}^n f_{q,c}^{\mathrm{REP}},\ f_{q,d,n}^{\mathrm{CHK}} \triangleq \bigodot_{i=1}^n f_{q,d}^{\mathrm{CHK}},\ F_{q,n}^{\mathrm{RM}} \triangleq \bigodot_{i=1}^n F_q^{\mathrm{RM}}.$$

Considering the kernel of $F_{q,c,d,n}^{\mathrm{LD}}$, we thus obtain an ensemble of regular LDPC codes over $\mathbb{F}_q$, which is called a *random (c,d)-regular LDPC code over* $\mathbb{F}_q$ and is denoted by $\mathcal{C}_{q,c,d}^{(n)}$.[1] This ensemble was originally introduced in [8], [12], [13] by the method of bipartite graphs.

To see the connection of $F_{q,c,d,n}^{\mathrm{LD}}$ with a bipartite graph, we may regard each $f_{q,c}^{\mathrm{REP}}$ as a variable node with c sockets and each $f_{q,d}^{\mathrm{CHK}}$ as a check node with d sockets. Then in total there are nc variable sockets and nc check sockets. We say that the ith variable socket and the jth check socket are connected by an edge if $j = \Pi(i)$, where Π is the random permutation defined in Definition 3.4. We also define the label of the edge connecting these two sockets to be the random variable C defined in Definition 3.3. Then we dispose of the sockets (i.e. edges are considered as connections between variable nodes and check nodes). The resulting random graph (which may have repeated edges) is exactly the random regular bipartite graph with independent and uniformly distributed random edge labels taken from $\mathbb{F}_q^\times$ as in [8].

[1] We shall tacitly assume throughout the paper that the block length n always takes values such that d divides cn.

Now let us investigate the weight distribution of $\mathcal{C}_{q,c,d}^{(n)}$. The next theorem gives its average weight distribution.

Theorem 3.6 (cf. [8], [9], [11]): For $c, d \in \mathbb{N}$, the average weight distribution of $\mathcal{C}_{q,c,d}^{(n)}$ is given by

$$E\Big[A_{q,c,d}^{(n)}(l)\Big] = \frac{\binom{n}{l} \operatorname{coef}\left(g_{q,d}^{(cn/d)}(x), x^{cl}\right)}{\binom{cn}{cl}(q-1)^{(c-1)l}} \tag{2}$$

where $A_{q,c,d}^{(n)}(l)$ denotes the number of codewords of weight l in $\mathcal{C}_{q,c,d}^{(n)}$ ($0 \le l \le n$), $\operatorname{coef}\left(p(x), x^l\right)$ denotes the coefficient of x^l in the polynomial $p(x)$, and

$$g_{q,d}^{(n)}(x) \triangleq \frac{1}{q^n}\left\{[1+(q-1)x]^d + (q-1)(1-x)^d\right\}^n. \tag{3}$$

Furthermore, we have

$$\frac{1}{n}\ln E\Big[A_{q,c,d}^{(n)}(l)\Big] \le \omega_{q,c,d}\left(\frac{l}{n}\right) + c\beta_{cn}(cl) \tag{4}$$

where

$$\omega_{q,c,d}(x) \triangleq H_q(x) + \frac{c}{d}\left[\delta_{q,d}(x) - \ln q\right] \tag{5}$$

$$\delta_{q,d}(x) \triangleq \inf_{\hat{x}\in(0,1)} \delta_{q,d}(x,\hat{x}) \tag{6}$$

$$\delta_{q,d}(x,\hat{x}) \triangleq dD(x\|\hat{x}) + \rho_{q,d}(\hat{x}) \tag{7}$$

$$\rho_{q,d}(x) \triangleq \ln\left[1 + (q-1)\left(1 - \frac{qx}{q-1}\right)^d\right] \tag{8}$$

$$\beta_n(l) \triangleq H_2\left(\frac{l}{n}\right) - \frac{1}{n}\ln\binom{n}{l}. \tag{9}$$

Proof: The average weight distribution (2) is in fact a known result. Note that

$$E\Big[A_{q,c,d}^{(n)}(l)\Big] = \binom{n}{l}(q-1)^l P\Big\{\mathbf{c}\in\mathcal{C}_{q,c,d}^{(n)}\Big|\, w(\mathbf{c}) = l\Big\}$$

and

$$P\Big\{\mathbf{c}\in\mathcal{C}_{q,c,d}^{(n)}\Big|\, w(\mathbf{c}) = l\Big\} = \frac{\left|\left\{\hat{\mathbf{c}}\in\ker f_{q,d,cn/d}^{\mathrm{CHK}} : w(\hat{\mathbf{c}}) = cl\right\}\right|}{\binom{cn}{cl}(q-1)^{cl}}.$$

For a proof of

$$\left|\left\{\hat{\mathbf{c}}\in\ker f_{q,d,cn/d}^{\mathrm{CHK}} : w(\hat{\mathbf{c}}) = cl\right\}\right| = \operatorname{coef}\left(g_{q,d}^{(cn/d)}(x), x^{cl}\right)$$

the reader is referred to [8, Appendix III], [9], [11].

Now let us prove the inequality (4). By the upper-bound technique introduced in Section I, it follows from (2) that

$$E\Big[A_{q,c,d}^{(n)}(l)\Big] \le \frac{\binom{n}{l} g_{q,d}^{(cn/d)}(x)}{\binom{cn}{cl}(q-1)^{(c-1)l} x^{cl}}$$

for any $x > 0$. Taking

$$x = \frac{\hat{x}}{(q-1)(1-\hat{x})}$$

where $\hat{x}\in(0,1)$, we obtain

$$E\Big[A_{q,c,d}^{(n)}(l)\Big] \le \frac{(q-1)^l\binom{n}{l}\hat{g}_{q,d}^{(cn/d)}(\hat{x})}{\binom{cn}{cl}\hat{x}^{cl}(1-\hat{x})^{cn-cl}} \tag{10}$$

where

$$\hat{g}_{q,d}^{(n)}(x) \triangleq \frac{1}{q^n}\left[1 + (q-1)\left(1 - \frac{qx}{q-1}\right)^d\right]^n.$$

Taking logarithms of both sides of (10) and using the lower-bound in Lemma A.1, we further have

$$\frac{1}{n}\ln E\Big[A_{q,c,d}^{(n)}(l)\Big] \le H_q(\alpha) + \frac{c}{d}\left[\delta_{q,d}(\alpha,\hat{x}) - \ln q\right] + c\beta_{cn}(cl)$$

where $\alpha \triangleq l/n$. The theorem is finally established by taking the infimum of the right side over all $\hat{x}\in(0,1)$. □

Remark 3.7: Loosely speaking, for any $\alpha\in[0,1]$, if we take $l = \alpha n$, then it follows from [4, Theorem 1] that

$$\begin{aligned}\lim_{n\to\infty}\frac{1}{n}\ln\operatorname{coef}\left(g_{q,d}^{(cn/d)}(x), x^{cl}\right) &= \frac{c}{d}\inf_{x>0}\ln\frac{g_{q,d}^{(1)}(x)}{x^{d\alpha}}\\ &= \inf_{x>0}\frac{1}{m}\ln\frac{g_{q,d}^{(cm/d)}(x)}{x^{cm\alpha}}\end{aligned}$$

for any $m > 0$. Comparing this identity with the proof of Theorem 3.6 and noting that the second term in the right hand side of (4) is asymptotically negligible, we immediately have

$$\lim_{n\to\infty}\frac{1}{n}\ln E\Big[A_{q,c,d}^{(n)}(\alpha n)\Big] = \omega_{q,c,d}(\alpha).$$

The function $\omega_{q,c,d}(x)$ thus represents the asymptotic growth rate of the average weight distribution of $\mathcal{C}_{q,c,d}^{(n)}$, and hence deserves further investigations. In the subsequent sections, we shall provide an in-depth analysis of $\omega_{q,c,d}(x)$.

Although in general the average weight distribution of $\mathcal{C}_{q,c,d}^{(n)}$ is very complex, it becomes simple for some special d. The next two theorems give its complete characterization for $d = 1, 2$.

Theorem 3.8:

$$E\Big[A_{q,c,1}^{(n)}(l)\Big] = \begin{cases} 1 & l = 0\\ 0 & \text{otherwise.}\end{cases}$$

Proof: For $d = 1$, we have $F_{q,c,d,n}^{\mathrm{LD}} = F_{q,cn}^{\mathrm{RM}}\circ\Sigma_{q,cn}\circ f_{q,c,n}^{\mathrm{REP}}$, which is injective. In other words, the defining parity-check matrix of $\mathcal{C}_{q,c,1}^{(n)}$ has rank n, so that $\mathcal{C}_{q,c,1}^{(n)} = \{\mathbf{0}\}$. □

Theorem 3.9:

$$E\Big[A_{q,c,2}^{(n)}(l)\Big] = \begin{cases} \frac{\binom{n}{l}\binom{cn/2}{cl/2}}{(q-1)^{(c/2-1)l}\binom{cn}{cl}} & cl \text{ is even}\\ 0 & \text{otherwise}\end{cases} \tag{11}$$

$$\frac{1}{n}\ln E\Big[A_{q,c,2}^{(n)}(l)\Big] \le \left(1 - \frac{c}{2}\right)H_q\left(\frac{l}{n}\right) + c\beta_{cn}(cl). \tag{12}$$

Proof: By (3) it follows that

$$g_{q,2}^{(n)}(x) = \left[1 + (q-1)x^2\right]^n.$$

Then we have

$$\operatorname{coef}\left(g_{q,2}^{(cn/2)}(x), x^{cl}\right) = \begin{cases} (q-1)^{cl/2}\binom{cn/2}{cl/2} & cl \text{ is even}\\ 0 & \text{otherwise.}\end{cases}$$

This together with (2) gives (11), which further yields (12) by Lemma A.1. □

As shown above, the average weight distribution of $\mathcal{C}_{q,c,d}^{(n)}$ is trivial for $d = 1, 2$. In the sequel, we shall therefore concentrate on the general case of $d \ge 3$.

Another well-known fact to be noted is that when $q = 2$ and d is even, the weight distribution of $\mathcal{C}^{(n)}_{q,c,d}$ satisfies $A^{(n)}_{2,c,d}(l) = A^{(n)}_{2,c,d}(n-l)$ for $0 \le l \le n$. This property simply follows from the fact that for even d the all-one vector is a codeword of $\mathcal{C}^{(n)}_{2,c,d}$. In particular we have the following:

Remark 3.10: For even $d \ge 2$,

$$E\Big[A^{(n)}_{2,c,d}(l)\Big] = E\Big[A^{(n)}_{2,c,d}(n-l)\Big] \tag{13}$$

$$\omega_{2,c,d}(x) = \omega_{2,c,d}(1-x). \tag{14}$$

We close this section with a theorem on the asymptotic behavior of the average weight distribution for the small-weight case.

Theorem 3.11: For $d \ge 3$ and constant weight $l \ge 1$,

$$E\Big[A^{(n)}_{q,c,d}(l)\Big] = \begin{cases} 0 & c = 1 \text{ and } l = 1 \\ 0 & q = 2 \text{ and } cl \text{ is odd} \\ \Theta\left(n^{-\lceil (c-2)l/2 \rceil}\right) & \text{otherwise.} \end{cases}$$

Proof: The trick of the proof is to find a precise approximation of $\operatorname{coef}(g^{(cn/d)}_{q,d}(x), x^{cl})$ in (2) and to prove it by induction. For convenience, we define

$$A(n,m) \triangleq \operatorname{coef}\left(g^{(n)}_{q,d}(x), x^m\right).$$

After some algebraic manipulations, we have

$$g^{(n)}_{q,d}(x) = \left[\sum_{i=0}^{d} \binom{d}{i} B(i) x^i\right]^n$$

where

$$B(i) = \frac{(q-1)^i + (-1)^i (q-1)}{q}.$$

Then it is observed that

$$\begin{aligned} A(n+1,m) &= \sum_{i=0}^{\min\{m,d\}} \binom{d}{i} A(n, m-i) B(i) \\ &= A(n,m) + \sum_{i=2}^{\min\{m,d\}} \binom{d}{i} A(n, m-i) B(i). \end{aligned}$$

Hence we have

$$\begin{aligned} A(n,0) &= A(1,0) = 1 \\ A(n,1) &= A(1,1) = 0 \\ A(n,2) &= A(n-1,2) + \binom{d}{2} A(n-1,0) B(2) \\ &= A(n-1,2) + \frac{d(d-1)(q-1)}{2} \\ &= \Theta\left(n^{\lfloor \frac{2}{2} \rfloor}\right) \\ A(n,3) &= A(n-1,3) + \binom{d}{2} A(n-1,1) B(2) \\ &\quad + \binom{d}{3} A(n-1,0) B(3) \\ &= A(n-1,3) + \frac{d(d-1)(d-2)(q-1)(q-2)}{6} \\ &= \begin{cases} 0 & q = 2 \\ \Theta\left(n^{\lfloor \frac{3}{2} \rfloor}\right) & \text{otherwise.} \end{cases} \end{aligned}$$

We shall show by induction on m that

$$A(n,m) = \begin{cases} 0 & q = 2 \text{ and } m \text{ is odd} \\ \Theta\left(n^{\lfloor \frac{m}{2} \rfloor}\right) & \text{otherwise.} \end{cases} \tag{15}$$

for all constant $m \ge 2$. Here, we only prove the general case of $q > 2$. The case of $q = 2$ can be proved by a similar argument with the fact $B(i) = [1 + (-1)^i]/2$. Suppose that (15) holds for $2 \le m \le k$ with $k \ge 3$, then for $m = k+1$,

$$\begin{aligned} A(n,k+1) &= A(n-1,k+1) \\ &\quad + \sum_{i=2}^{\min\{k+1,d\}} \binom{d}{i} A(n-1, k-i+1) B(i) \\ &= A(n-1,k+1) + \Theta\left((n-1)^{\lfloor (k-1)/2 \rfloor}\right) \end{aligned}$$

This asymptotic behavior implies that there exits a positive integer n_0 such that for $n > n_0$,

$$\begin{aligned} A(n,k+1) &= A(n_0,k+1) + \Theta\left(\sum_{i=n_0}^{n-1} i^{\lfloor (k-1)/2 \rfloor}\right) \\ &= \Theta\left(n^{\lfloor (k+1)/2 \rfloor}\right). \end{aligned}$$

Thus (15) holds for all $m \ge 2$.

Finally, it follows from Theorem 3.6 and (15) that

$$\begin{aligned} E\Big[A^{(n)}_{q,c,d}(l)\Big] &= \frac{\binom{n}{l} A(cn/d, cl)}{\binom{cn}{cl} (q-1)^{(c-1)l}} \\ &= \begin{cases} 0 & c = 1 \text{ and } l = 1 \\ 0 & q = 2 \text{ and } cl \text{ is odd} \\ \Theta\left(n^{-\lceil (c-2)l/2 \rceil}\right) & \text{otherwise} \end{cases} \end{aligned}$$

as desired. □

Remark 3.12: The first and second cases of Theorem 3.11 have the following alternative proofs: If $c = 1$ then the random code $\mathcal{C}^{(n)}_{q,c,d}$, as the kernel of the reduced mapping $f^{\mathrm{CHK}}_{q,d,n/d} \circ F^{\mathrm{RM}}_{q,n} \circ \Sigma_{q,n}$, has the same weight distribution as the kernel of $f^{\mathrm{CHK}}_{q,d,n/d}$. In particular, $\mathcal{C}^{(n)}_{q,c,d}$ has no words of weight 1. If c is odd then every column of the parity-check matrix of $\mathcal{C}^{(n)}_{2,c,d}$ (i.e. the transformation matrix of $F^{\mathrm{LD}}_{2,c,d,n}$) has odd weight. This implies that the all-one vector is in the dual code of $\mathcal{C}^{(n)}_{2,c,d}$ and hence that all codewords have even weight.

IV. Properties of the Function $\delta_{q,d}(x)$

As an important step towards understanding the function $\omega_{q,c,d}(x)$, we analyze in this section the function $\delta_{q,d}(x)$ defined by (6). The proofs of lemmas in this section are presented in Appendix D.

In the sequel, we shall frequently use the following substitution to facilitate the analysis:

$$z \triangleq 1 - \frac{qx}{q-1}, \quad \hat{z} \triangleq 1 - \frac{q\hat{x}}{q-1}. \tag{16}$$

Note that this transform is bijective and strictly decreasing, so we have

$$x = \frac{(q-1)(1-z)}{q}, \quad \hat{x} = \frac{(q-1)(1-\hat{z})}{q} \tag{17}$$

and $z, \hat{z} \in [-1/(q-1), 1]$ as $x, \hat{x} \in [0,1]$.

Our first goal is to study the zeros of the partial derivative of $\delta_{q,d}(x,\hat{x})$ with respect to $\hat{x}$.

Lemma 4.1: For the function $\delta_{q,d}(x,\hat{x})$ defined by (7),

$$\frac{\partial \delta_{q,d}(x,\hat{x})}{\partial \hat{x}} = d\frac{\partial D(x\|\hat{x})}{\partial \hat{x}} + \frac{d\rho_{q,d}(\hat{x})}{d\hat{x}} \tag{18}$$

$$= -\frac{qd(\zeta_{q,d}(\hat{z})-z)}{(1-\hat{z})[1+(q-1)\hat{z}]} \tag{19}$$

where

$$\zeta_{q,d}(\hat{z}) \triangleq \frac{\hat{z}+\hat{z}^{d-1}+(q-2)\hat{z}^d}{1+(q-1)\hat{z}^d}. \tag{20}$$

Lemma 4.1 shows that the zeros of $\partial\delta_{q,d}(x,\hat{x})/\partial\hat{x}$ are determined by the equation $\zeta_{q,d}(\hat{z})-z=0$. We therefore proceed to analyze the function $\zeta_{q,d}(\hat{z})$. The next three lemmas give the properties of $\zeta_{q,d}(\hat{z})$.

Lemma 4.2: For $q \geq 2$ and $d \geq 3$, the function $\zeta_{q,d}(\hat{z})$ is continuously differentiable on $[-1/(q-1),1]$ and its derivative is positive on $(-1/(q-1),1)$.

Lemma 4.3: For $q \geq 2$ and $d \geq 1$,

$$\zeta_{q,d}(z) - z = \frac{z^{d-1}(1-z)[1+(q-1)z]}{1+(q-1)z^d} \tag{21}$$

$$\zeta_{q,d}\left(-\frac{1}{q-1}\right) = \begin{cases} \frac{2}{d}-1 & q=2 \text{ and } d \text{ is odd} \quad (22a) \\ -\frac{1}{q-1} & \text{otherwise} \quad (22b) \end{cases}$$

$$\zeta_{q,d}(0) = 0 \tag{23}$$

$$\zeta_{q,d}(1) = 1. \tag{24}$$

Lemma 4.4: Let

$$z_1 \triangleq \begin{cases} \dfrac{2}{d}-1 & q=2 \text{ and } d \text{ is odd} \quad (25a) \\ -\dfrac{1}{q-1} & \text{otherwise.} \quad (25b) \end{cases}$$

The equation $\zeta_{q,d}(\hat{z})-z=0$ has a unique solution $\hat{z}_1=\hat{z}_1(z)$ in $[-1/(q-1),1]$ for each $z\in[z_1,1]$ and has no solution in $[-1/(q-1),1]$ for $z<z_1$. The solution $\hat{z}_1(z)$ is continuous on $[z_1,1]$ and is continuously differentiable on $(z_1,1)$; its derivative is positive on $(z_1,1)$. Moreover, $\hat{z}_1(z)\in I'_{q,d}(z)$, where

$$I'_{q,d}(z) \triangleq \begin{cases} \{-\frac{1}{q-1}\} & z=z_1 \\ (-\frac{1}{q-1},z) & z\in(z_1,0) \text{ and } d \text{ is odd} \\ (z,0) & z\in(z_1,0) \text{ and } d \text{ is even} \\ \{0\} & z=0 \\ (0,z) & z\in(0,1) \\ \{1\} & z=1. \end{cases}$$

Equipped with Lemmas 4.1–4.4, we are now in a position to analyze the function $\delta_{q,d}(x)$.

Theorem 4.5: Let $q\geq 2$, $d\geq 3$, and

$$x_1 \triangleq \begin{cases} 1-\dfrac{1}{d} & q=2 \text{ and } d \text{ is odd} \quad (26a) \\ 1 & \text{otherwise.} \quad (26b) \end{cases}$$

For the function $\delta_{q,d}(x)$ defined by (6), we have

$$\delta_{q,d}(x) = \begin{cases} \ln q & x=0 \quad (27a) \\ \rho_{q,d}(1) & x=1 \quad (27b) \\ -\infty & x\in(1-\frac{1}{d},1),\ q=2, \\ & \text{and } d \text{ is odd} \quad (27c) \\ \ln(2d)-dH_2\left(\dfrac{1}{d}\right) & x=1-\frac{1}{d},\ q=2, \\ & \text{and } d \text{ is odd} \quad (27d) \\ \delta_{q,d}(x,\hat{x}_1) & x\in(0,x_1) \quad (27e) \end{cases}$$

where $\rho_{q,d}(x)$ is defined by (8) and $\hat{x}_1=\hat{x}_1(x)$ is the unique root in $(0,1)$ of the equation

$$\frac{\partial\delta_{q,d}(x,\hat{x})}{\partial\hat{x}} = 0 \tag{28}$$

solved for $\hat{x}$ as a function of x. The function $\hat{x}_1(x)$ is continuously differentiable on $(0,x_1)$ and its derivative is positive on $(0,x_1)$. Moreover, $\lim_{x\to 0^+}\hat{x}_1(x)=0$, $\lim_{x\to x_1^-}\hat{x}_1(x)=1$, and $\hat{x}_1(x)\in I_{q,d}(x)$, where

$$I_{q,d}(x) \triangleq \begin{cases} (x,1-\frac{1}{q}) & x\in(0,1-\frac{1}{q}) \\ \{1-\frac{1}{q}\} & x=1-\frac{1}{q} \\ (x,1) & x\in(1-\frac{1}{q},x_1) \text{ and } d \text{ is odd} \\ (1-\frac{1}{q},x) & x\in(1-\frac{1}{q},x_1) \text{ and } d \text{ is even.} \end{cases}$$

The function $\delta_{q,d}(x)$ is continuous on $[0,x_1]$ and is continuously differentiable on $(0,x_1)$, in which case,

$$\frac{d\delta_{q,d}(x)}{dx} = d\ln\frac{x(1-\hat{x}_1)}{\hat{x}_1(1-x)}. \tag{29}$$

Proof: At first, Lemmas 4.1, 4.2, and 4.3 show that

$$\frac{\partial\delta_{q,d}(0,\hat{x})}{\partial\hat{x}} > 0 \qquad \forall\hat{x}\in(0,1)$$

and

$$\frac{\partial\delta_{q,d}(1,\hat{x})}{\partial\hat{x}} < 0 \qquad \forall\hat{x}\in(0,1).$$

Therefore we have

$$\delta_{q,d}(0) = \lim_{\hat{x}\to 0^+}\delta_{q,d}(0,\hat{x}) = \rho_{q,d}(0)$$

and

$$\delta_{q,d}(1) = \lim_{\hat{x}\to 1^-}\delta_{q,d}(1,\hat{x}) = \rho_{q,d}(1).$$

This concludes (27a) and (27b).

A similar argument also shows that for odd d

$$\frac{\partial\delta_{2,d}(x,\hat{x})}{\partial\hat{x}} < 0 \qquad \forall x\in\left[1-\frac{1}{d},1\right), \hat{x}\in(0,1)$$

so that

$$\begin{aligned} \delta_{2,d}(x) &= \lim_{\hat{x}\to 1^-}\delta_{2,d}(x,\hat{x}) \\ &= -dH_2(x) + \lim_{\hat{x}\to 1^-}\ln\frac{1+(1-2\hat{x})^d}{(1-\hat{x})^{d(1-x)}} \\ &= -dH_2(x) + \ln\lim_{\hat{x}\to 1^-}\frac{2(1-2\hat{x})^{d-1}}{(1-x)(1-\hat{x})^{d(1-x)-1}} \\ &= -dH_2(x) + \ln\frac{2}{(1-x)\lim_{\hat{x}\to 1^-}(1-\hat{x})^{d-1-dx}} \end{aligned}$$

which yields (27c) and (27d).

For $x \in (0, x_1)$, Lemma 4.4 shows that there is a unique $\hat{z}_1 = \hat{z}_1(z) \in (-1/(q-1), 1)$ such that $\zeta_{q,d}(\hat{z}_1) = z = 1 - qx/(q-1)$. Let $\hat{x}_1 = (q-1)(1-\hat{z}_1)/q$, which is essentially a function of x. Then it follows from Lemma 4.1 and 4.2 that

$$\frac{\partial \delta_{q,d}(x, \hat{x})}{\partial \hat{x}} < 0 \qquad \forall \hat{x} \in (0, \hat{x}_1)$$

and

$$\frac{\partial \delta_{q,d}(x, \hat{x})}{\partial \hat{x}} > 0 \qquad \forall \hat{x} \in (\hat{x}_1, 1).$$

Therefore, $\delta_{q,d}(x) = \delta_{q,d}(x, \hat{x}_1)$, which concludes (27e). Furthermore, Lemma 4.4 shows that $\hat{x}_1(x)$ is continuously differentiable on $(0, x_1)$ and its derivative is positive on $(0, x_1)$. It also shows that $\lim_{x \to 0^+} \hat{x}_1(x) = 0$ and $\lim_{x \to x_1^-} \hat{x}_1(x) = 1$, and that $\hat{x}_1(x) \in I_{q,d}(x)$.

Based on the above analysis, it is clear that $\delta_{q,d}(x)$ is continuously differentiable on $(0, x_1)$. Furthermore, equation (27e) combined with Lemma B.1 gives (29).

Finally, let us show that $\delta_{q,d}(x)$ is continuous at the endpoints of the interval. Note that $\delta_{q,d}(x)$ is the infimum of a collection of continuous functions, so it is upper semi-continuous. Then it suffices to show that $\lim_{x \to 0^+} \delta_{q,d}(x) \geq \delta_{q,d}(0)$ and $\lim_{x \to x_1^-} \delta_{q,d}(x) \geq \delta_{q,d}(x_1)$. Recall that $\lim_{x \to 0^+} \hat{x}_1(x) = 0$ and $\lim_{x \to x_1^-} \hat{x}_1(x) = 1$, so we have

$$\lim_{x \to 0^+} \delta_{q,d}(x) \geq \lim_{x \to 0^+} \rho_{q,d}(\hat{x}_1(x)) = \ln q$$

$$\lim_{x \to x_1^-} \delta_{q,d}(x) \geq \lim_{x \to x_1^-} \rho_{q,d}(\hat{x}_1(x)) = \rho_{q,d}(1)$$

and

$$\begin{aligned} \lim_{x \to x_1^-} \delta_{2,d}(x) &\geq \lim_{x \to x_1^-} \left[-dH_2(x) + \ln \frac{1 + (1 - 2\hat{x}_1(x))^d}{1 - \hat{x}_1(x)} \right] \\ &= \ln(2d) - dH_2\left(\frac{1}{d}\right) \end{aligned}$$

for odd d. The proof is complete. □

In Fig. 1 we give an illustration of the graphs of $\delta_{q,d}(x)$ for $(q,d) = (2,5)$, $(q,d) = (2,6)$, $(q,d) = (3,5)$, and $(q,d) = (3,6)$.

V. Properties of the Function $\omega_{q,c,d}(x)$

In this section, we proceed to analyze the properties of the function $\omega_{q,c,d}(x)$ defined by (5). Since LDPC codes are trivial when $c > d$, we shall sometimes assume $c \leq d$ to exclude trivial cases. The proofs of lemmas in this section are presented in Appendix E.

At first, we calculate the value of $\omega_{q,c,d}(x)$ at some special points.

Lemma 5.1: Let $q \geq 2$, $c \geq 1$, and $d \geq 3$.

$$\omega_{q,c,d}(0) = 0. \tag{30}$$

$$\omega_{q,c,d}\left(1 - \frac{1}{q}\right) = \left(1 - \frac{c}{d}\right) \ln q. \tag{31}$$

$$\omega_{q,c,d}(1) = \ln(q-1) + \frac{c}{d}\rho_{q,d}(1) - \frac{c}{d} \ln q. \tag{32}$$

If $q = 2$ and d is odd then

$$\omega_{q,c,d}\left(1 - \frac{1}{d}\right) = (1 - c)\, H_2\left(\frac{1}{d}\right) + \frac{c}{d} \ln d \tag{33}$$

and

$$\omega_{q,c,d}(x) = -\infty \qquad \forall x \in \left(1 - \frac{1}{d}, 1\right). \tag{34}$$

Lemma 5.1 is an easy consequence of Theorem 4.5, so its proof is left to the reader. Next, let us calculate the first-order derivative of $\omega_{q,c,d}(x)$.

Lemma 5.2: For the function $\omega_{q,c,d}(x)$ defined by (5) with $q \geq 2$, $c \geq 1$, and $d \geq 3$, if x belongs to the case (27e) then

$$\frac{d\omega_{q,c,d}(x)}{dx} = \ln \left[\left(\frac{x}{1-x}\right)^{c-1} \left(\frac{1 - \hat{x}_1}{\hat{x}_1}\right)^{c} \right] + \ln(q-1) \tag{35}$$

which can be further expressed as

$$\frac{d\omega_{q,c,d}(x)}{dx} = \ln \left\{ \frac{1 + (q-1)\hat{z}_1}{1 - \hat{z}_1} \left[\frac{1 - \hat{z}_1^{d-1}}{1 + (q-1)\hat{z}_1^{d-1}} \right]^{c-1} \right\} \tag{36}$$

where $\hat{x}_1$ is defined by (28) and $\hat{z}_1 = 1 - q\hat{x}_1/(q-1)$.

The next lemma gives the value of $d\omega_{q,c,d}(x)/dx$ at some special points.

Lemma 5.3: Let $q \geq 2$, $d \geq 3$, and x_1 be defined by (26).

$$\lim_{x \to 0^+} \frac{d\omega_{q,c,d}(x)}{dx} = \begin{cases} \infty & c = 1 \quad (37\text{a}) \\ \ln(d-1) & c = 2 \quad (37\text{b}) \\ -\infty & c \geq 3. \quad (37\text{c}) \end{cases}$$

$$\left. \frac{d\omega_{q,c,d}(x)}{dx} \right|_{x = 1 - \frac{1}{q}} = 0. \tag{38}$$

If $q = 2$ and d is even then

$$\lim_{x \to 1^-} \frac{d\omega_{q,c,d}(x)}{dx} = \begin{cases} -\infty & c = 1 \quad (39\text{a}) \\ -\ln(d-1) & c = 2 \quad (39\text{b}) \\ \infty & c \geq 3. \quad (39\text{c}) \end{cases}$$

If $q \neq 2$ or d is odd then

$$\lim_{x \to x_1^-} \frac{d\omega_{q,c,d}(x)}{dx} = -\infty. \tag{40}$$

To have more insights into $\omega_{q,c,d}(x)$, we proceed to analyze the second-order derivative of $\omega_{q,c,d}(x)$. Since

$$\frac{d^2\omega_{q,c,d}(x)}{dx^2} = \frac{d}{d\hat{z}_1}\left(\frac{d\omega_{q,c,d}(x)}{dx}\right) \cdot \frac{d\hat{z}_1}{dx} \tag{41}$$

and we note that

$$\frac{d\hat{z}_1}{dx} = -\frac{q}{q-1}\frac{d\hat{x}_1}{dx}$$

is negative on $(0, x_1)$, our task is now to calculate the derivative $d(d\omega_{q,c,d}(x)/dx)/d\hat{z}_1$.

Lemma 5.4: For the function $\omega_{q,c,d}(x)$ defined by (5) with $q \geq 2$, $c \geq 1$, and $d \geq 3$, if x belongs to the case (27e) then

$$\begin{aligned} &\frac{d}{d\hat{z}_1}\left(\frac{d\omega_{q,c,d}(x)}{dx}\right) \\ &= \frac{q\xi_{q,c,d}(\hat{z}_1)}{(1 - \hat{z}_1^{d-1})[1 + (q-1)\hat{z}_1][1 + (q-1)\hat{z}_1^{d-1}]} \end{aligned} \tag{42}$$

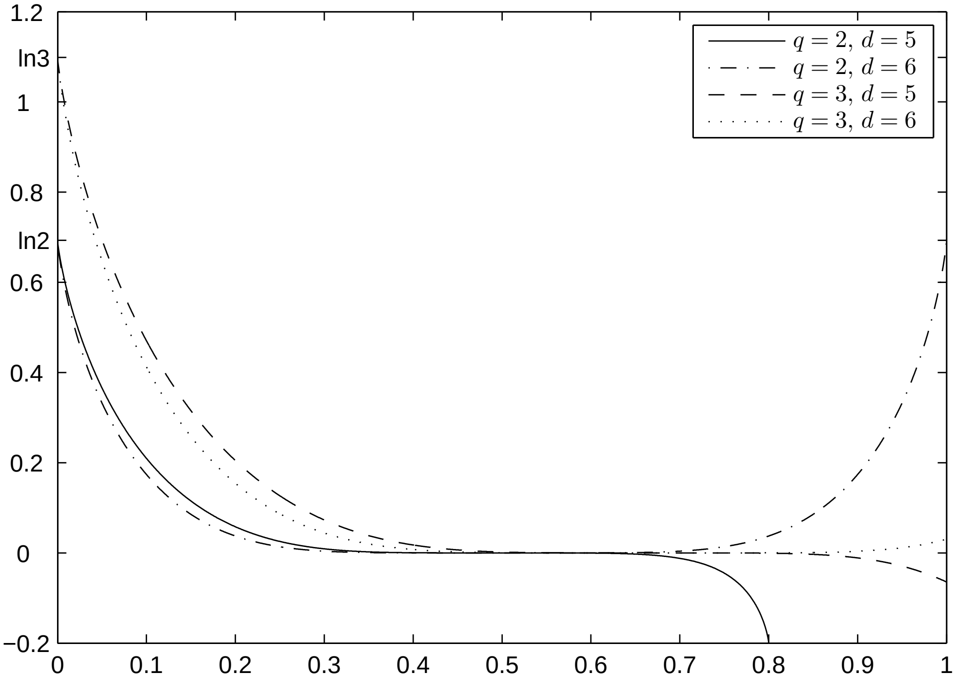

Fig. 1. The graphs of $\delta_{q,d}(x)$ for $(q,d) = (2,5)$, $(q,d) = (2,6)$, $(q,d) = (3,5)$, and $(q,d) = (3,6)$.

where

$$\xi_{q,c,d}(\hat{z}) = \sum_{i=0}^{d-3} \hat{z}^i - [(c-1)(d-1)-1]\hat{z}^{d-2} - (q-1)[(c-1)(d-1)-1]\hat{z}^{d-1} + (q-1)\sum_{i=d}^{2d-3} \hat{z}^i. \tag{43}$$

When $c = 1$, equation (42) reduces to

$$\frac{d}{d\hat{z}_1}\left(\frac{d\omega_{2,c,d}(x)}{dx}\right) = \frac{q}{(1-\hat{z}_1)[1+(q-1)\hat{z}_1]}. \tag{44}$$

We go on to analyze the function $\xi_{q,c,d}(\hat{z})$ for $q \geq 2$, $c \geq 2$, and $d \geq \max\{c, 3\}$.

Lemma 5.5: For $d \geq 3$, the function $\xi_{2,2,d}(\hat{z})$ is positive on $(-1, 1)$. For $q \geq 3$ and $d \geq 3$, the function $\xi_{q,2,d}(\hat{z})$ has a positive zero $\hat{z}_2$ in $(-1/(q-1), 1)$, and $\xi_{q,2,d}(\hat{z})$ is positive on $(-1/(q-1), \hat{z}_2)$ and negative on $(\hat{z}_2, 1)$.

For $d \geq c \geq 3$ with d even, the function $\xi_{2,c,d}(\hat{z})$ has one zero $\hat{z}_2$ in $(0, 1)$ and the other zero $\hat{z}_2'$ in $(-1, 0)$, and $\xi_{2,c,d}(\hat{z})$ is positive on $(\hat{z}_2', \hat{z}_2)$ and negative on $(-1, \hat{z}_2') \cup (\hat{z}_2, 1)$.

For $q \geq 2$ and $d \geq c \geq 3$ with $q \neq 2$ or d odd, the function $\xi_{q,c,d}(\hat{z})$ has a positive zero $\hat{z}_2$ in $(-1/(q-1), 1)$, and $\xi_{q,c,d}(\hat{z})$ is positive on $(-1/(q-1), \hat{z}_2)$ and negative on $(\hat{z}_2, 1)$.

We are now ready to give the qualitative properties of $\omega_{q,c,d}(x)$.

Theorem 5.6: Let $q \geq 2$, $c \geq 1$, $d \geq \max\{c, 3\}$, and x_1 be defined by (26). The function $\omega_{q,c,d}(x)$ defined by (5) is continuous on $[0, x_1]$ and is twice differentiable on $(0, x_1)$.

If $c = 1$, then $\omega_{q,c,d}(x)$ is concave on $(0, x_1)$, and it is strictly increasing on $(0, 1 - 1/q)$ and strictly decreasing on $(1 - 1/q, x_1)$.

If $c = 2$, then $\omega_{q,c,d}(x)$ is strictly increasing on $(0, 1-1/q)$ and strictly decreasing on $(1 - 1/q, x_1)$. Moreover, if $q = 2$, it is concave on $(0, x_1)$; otherwise, it is convex on $(0, x_2)$ and concave on $(x_2, 1)$, where $x_2 \in (0, 1 - 1/q)$.

If $c \geq 3$, $q = 2$, and d is even, then $\omega_{q,c,d}(x)$ is symmetric about the axis $x = \frac{1}{2}$. It is convex on $(0, x_2)$ and concave on $(x_2, \frac{1}{2})$ for some $x_2 \in (0, \frac{1}{2})$; it is strictly decreasing on $(0, x_3)$ and strictly increasing on $(x_3, \frac{1}{2})$, where $x_3 \in (0, x_2)$; consequently, it has a unique zero x_0 in $(0, \frac{1}{2}]$, where $x_0 \in (x_3, \frac{1}{2}]$, and it is negative on $(0, x_0)$ and positive on $(x_0, \frac{1}{2})$.

For other cases, the function $\omega_{q,c,d}(x)$ is convex on $(0, x_2)$ and concave on (x_2, x_1), where $x_2 \in (0, 1-1/q)$; it is strictly decreasing on $(0, x_3) \cup (1 - 1/q, x_1)$ and strictly increasing on $(x_3, \frac{1}{2})$, where $x_3 \in (0, x_2)$; consequently, it has a unique zero x_0 in $(0, 1 - 1/q]$, where $x_0 \in (x_3, 1 - 1/q]$, and it is negative on $(0, x_0)$ and positive on $(x_0, 1 - 1/q)$.

To provide an intuitive illustration of $\omega_{q,c,d}(x)$ in each case, the graphs of $\omega_{q,c,d}(x)$ for typical values of (q, c, d) are plotted in Figs. 2–5.

Sketch of Proof: The proof is direct, and it depends on Remark 3.10, Theorem 4.5, Lemmas 5.1–5.5, and identity (41). Here, we only give the proof of the last paragraph of statements.

Lemma 5.5 and identity (41) show that $\omega_{q,c,d}$ is convex on $(0, x_2)$ and concave on (x_2, x_1), where $x_2 \in (0, 1 - 1/q)$. Furthermore, Lemmas 5.1 and 5.3 show that

$$\omega_{q,c,d}(0) = 0, \quad \omega_{q,c,d}\left(1 - \frac{1}{q}\right) = \left(1 - \frac{c}{d}\right)\ln q \geq 0$$

and

$$\lim_{x \to 0^+} \frac{d\omega_{q,c,d}(x)}{dx} = -\infty, \quad \left.\frac{d\omega_{q,c,d}(x)}{dx}\right|_{x=1-\frac{1}{q}} = 0.$$

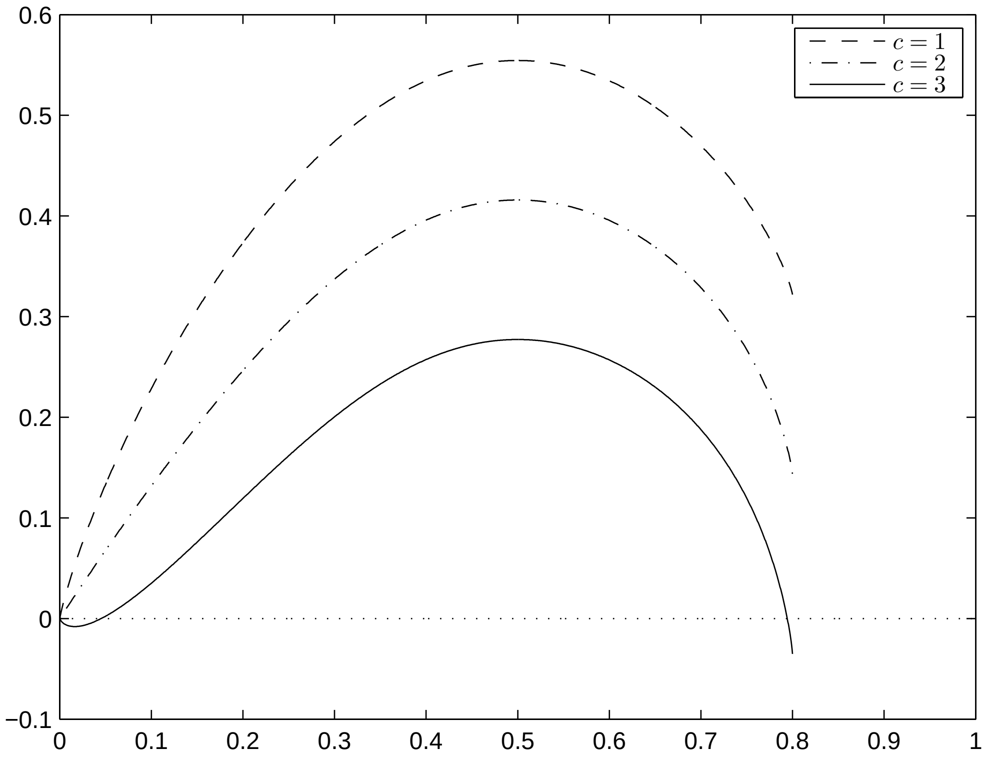

Fig. 2. The graphs of $\omega_{2,c,5}(x)$ for $c = 1$, $c = 2$, and $c = 3$.

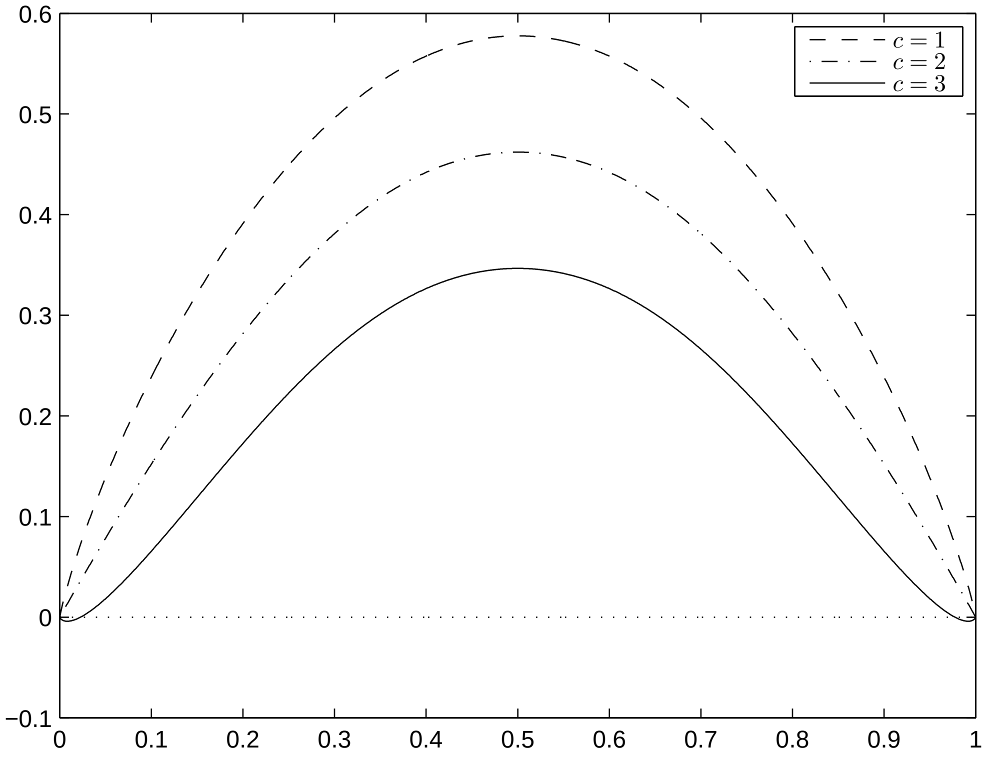

Fig. 3. The graphs of $\omega_{2,c,6}(x)$ for $c = 1$, $c = 2$, and $c = 3$.

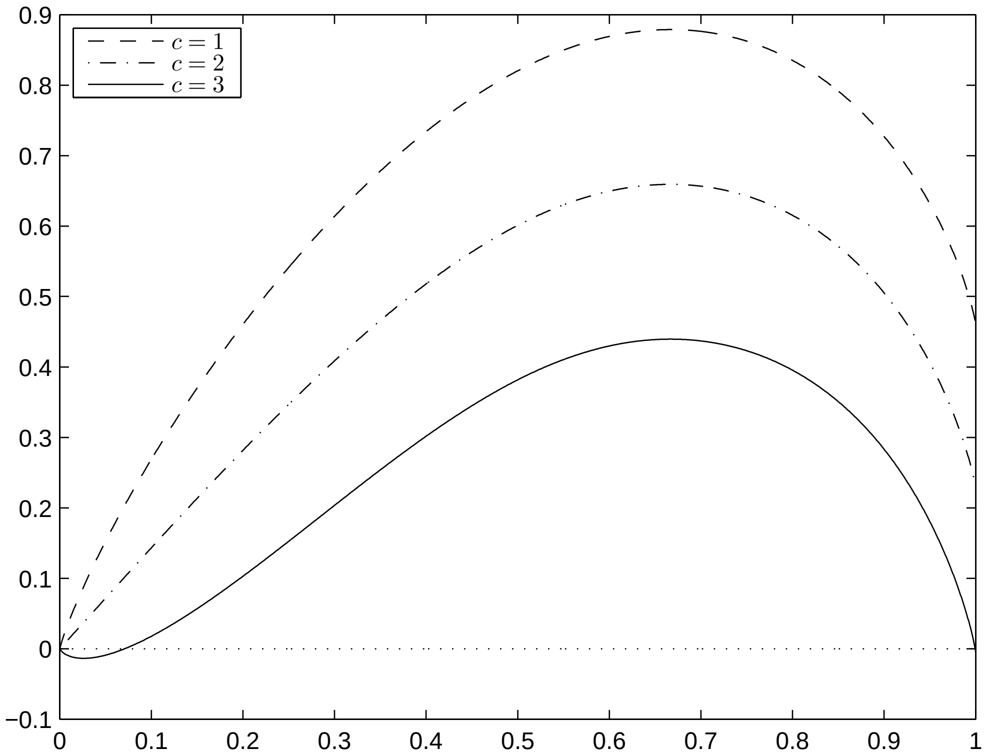

Fig. 4. The graphs of $\omega_{3,c,5}(x)$ for $c = 1$, $c = 2$, and $c = 3$.

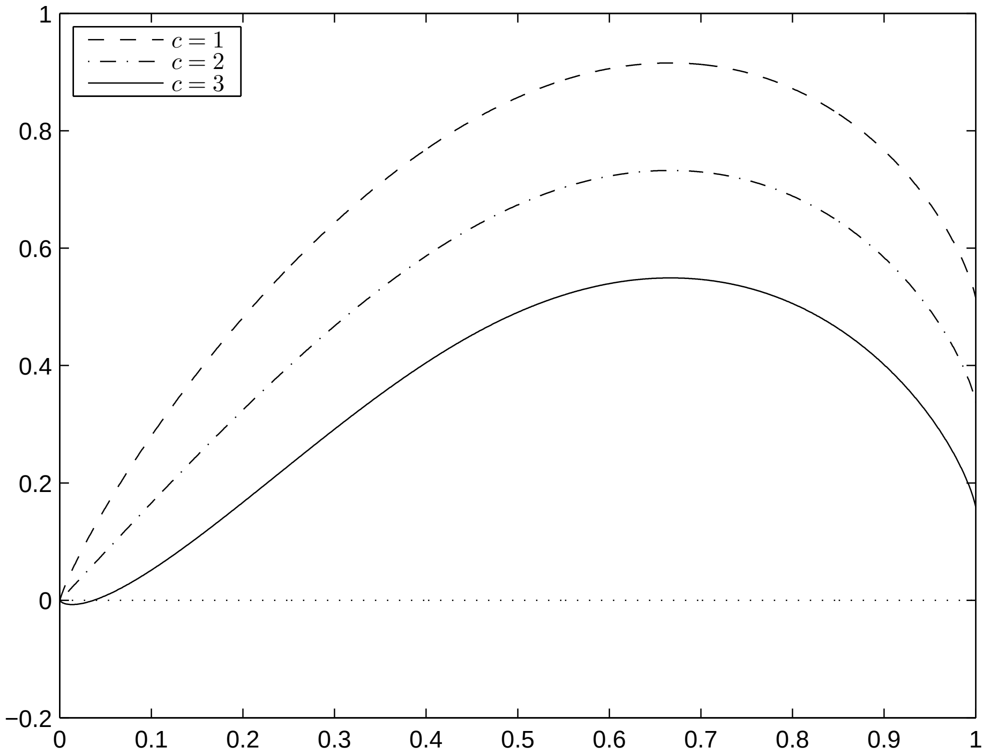

Fig. 5. The graphs of $\omega_{3,c,6}(x)$ for $c = 1$, $c = 2$, and $c = 3$.

Therefore, the derivative $d\omega_{q,c,d}(x)/dx$ has a unique zero x_3 in $(0, 1-1/q)$, where $x_3 \in (0, x_2)$; it is negative on $(0, x_3) \cup (1-1/q, x_1)$ and positive on $(x_3, 1-1/q)$. In other words, the function $\omega_{q,c,d}(x)$ is strictly decreasing on $(0, x_3) \cup (1-1/q, x_1)$ and strictly increasing on $(x_3, 1-1/q)$. The last statement about the unique zero in $(0, 1-1/q)$ clearly follows. □

Remark 5.7: The zero x_0 in Theorem 5.6 just corresponds to the normalized minimum distance of LDPC codes, in an average and asymptotic sense. It is in fact a function of q, c, and d, so we denote it by $x_0(q, c, d)$. We note that

$$\lim_{d\to\infty} \rho_{q,d}(x) = 0 \qquad \forall x \in (0,1)$$

and hence for any $r \in (0, 1]$,

$$\lim_{d\to\infty} x_0(q, \lceil rd \rceil, d) = x_{0,q,r}$$

where $x_{0,q,r}$ is the solution of $H_q(x) - r \ln q = 0$ in $(0, 1-1/q)$. The detailed proof is left to the reader. Note that $x_{0,q,r}$ as well as the equation $H_q(x) - r \ln q = 0$ is closely related to the so-called asymptotic Gilbert-Varshamov (GV) bound over finite fields [14, pp. 94–95]. This implies that regular LDPC codes with large c and d achieve the GV bound.

VI. Minimum Distance of LDPC Codes

Though we have shown in Remark 5.7 that regular LDPC code ensembles are asymptotically good, we are more interested in the performance of individual codes of finite length. In this section, we shall investigate the minimum distance of an individual code in a regular LDPC code ensemble. To achieve this goal, we first establish an important inequality.

Theorem 6.1: For $q \ge 2$, $c \ge 1$, $d \ge 2$, and $x \in (0, 1/q^2)$,

$$\omega_{q,c,d}(x) < \left(\frac{c}{2} - 1\right) x \ln x + \kappa_{q,c,d} x \tag{45}$$

where

$$\kappa_{q,c,d} \triangleq \ln(q-1) + \frac{c}{2}\ln(d-1) + 3c. \tag{46}$$

Proof: Put

$$\hat{x} \triangleq \sqrt{\frac{x}{d-1}}. \tag{47}$$

Then for any $x \in (0, 1/q^2)$, $\hat{x} \in (0, 1/q) \subset (0, 1-1/q)$.

According to the definition (5) of $\omega_{q,c,d}(x)$, we have

$$\begin{aligned}
&\omega_{q,c,d}(x)\\
&\quad \le H_q(x) + \frac{c}{d}(\delta_{q,d}(x,\hat{x}) - \ln q)\\
&\quad = H_q(x) + cD(x\|\hat{x})\\
&\qquad + \frac{c}{d}\ln\left[\frac{1}{q} + \left(1 - \frac{1}{q}\right)\left(1 - \frac{q\hat{x}}{q-1}\right)^d\right]\\
&\quad \overset{\text{(a)}}{\le} H_q(x) + cD(x\|\hat{x}) + c\left[-\hat{x} + \frac{q(d-1)}{2(q-1)}\hat{x}^2\right]\\
&\quad = -(c-1)H_2(x) + x\ln(q-1)\\
&\qquad + c\left[x \ln\frac{1}{\hat{x}} + (1-x)\ln\frac{1}{1-\hat{x}} - \hat{x} + \frac{q(d-1)}{2(q-1)}\hat{x}^2\right]\\
&\quad < (c-1)x\ln x + x\ln(q-1)\\
&\qquad + c\left[x\ln\frac{1}{\hat{x}} + \frac{\hat{x}}{1-\hat{x}} - \hat{x} + \frac{q(d-1)}{2(q-1)}\hat{x}^2\right]\\
&\quad = (c-1)x\ln x + x\ln(q-1)\\
&\qquad + c\left[x\ln\frac{1}{\hat{x}} + \frac{\hat{x}^2}{1-\hat{x}} + \frac{q(d-1)}{2(q-1)}\hat{x}^2\right]\\
&\quad \overset{\text{(b)}}{=} (c-1)x\ln x + x\ln(q-1)\\
&\qquad + c\left[\frac{1}{2}x\ln\frac{d-1}{x} + \frac{x}{(d-1)(1-\hat{x})} + \frac{qx}{2(q-1)}\right]\\
&\quad \overset{\text{(c)}}{<} \left(\frac{c}{2} - 1\right)x\ln x + \left(\ln(q-1) + \frac{c}{2}\ln(d-1) + 3c\right)x
\end{aligned}$$

where (a) follows from Lemma A.2 and $\ln x \le x - 1$, (b) from (47), and (c) follows from $q \ge 2$, $d \ge 2$, and $\hat{x} < 1/q$. □

Now, let us present the main result on the minimum distance of individual codes in a regular LDPC code ensemble.

Theorem 6.2: For any code $C \subseteq \mathbb{F}_q^n$, we denote its minimum distance by $\mathrm{d_{min}}(C)$. Then for $q \ge 2$, $d \ge c \ge 3$, $l_0 \ge 1$, and $\alpha \in (0, 1-1/q)$,

$$\begin{aligned}
&P\Big\{l_0 \le \mathrm{d_{min}}(\mathcal{C}_{q,c,d}^{(n)}) \le n\alpha\Big\}\\
&\qquad \le \Theta\left(n^{-\lceil (c-2)(l_0+\Delta)/2 \rceil}\right) + \Theta\left(n^{\frac{3}{2}} e^{n\omega_{q,c,d}(\alpha)}\right)
\end{aligned} \tag{48}$$

where

$$\Delta \triangleq \begin{cases} 1 & q = 2 \text{ and } cl_0 \text{ is odd}\\ 0 & \text{otherwise.}\end{cases} \tag{49}$$

Proof: Since the minimum distance of a linear code is the minimum weight of its nonzero codewords, we have

$$\begin{aligned}
&P\Big\{l_0 \le \mathrm{d_{min}}(\mathcal{C}_{q,c,d}^{(n)}) \le n\alpha\Big\}\\
&\quad \le P\left\{\bigcup_{l=l_0}^{\lfloor n\alpha \rfloor}\Big\{A_{q,c,d}^{(n)}(l) \ge 1\Big\}\right\}\\
&\quad \le \sum_{l=l_0}^{\lfloor n\alpha \rfloor} P\Big\{A_{q,c,d}^{(n)}(l) \ge 1\Big\}\\
&\quad \overset{\text{(a)}}{\le} \sum_{l=l_0}^{\lfloor n\alpha \rfloor} E\Big[A_{q,c,d}^{(n)}(l)\Big]\\
&\quad \overset{\text{(b)}}{\le} \sum_{l=l_0}^{l_0+3} \Theta\left(n^{-\lceil (c-2)l/2 \rceil}\right) + \sum_{l=l_0+4}^{\lfloor n\alpha \rfloor} \Theta\left(n^{\frac{1}{2}} e^{n\omega_{q,c,d}(l/n)}\right)\\
&\quad \overset{\text{(c)}}{\le} \Theta\left(n^{-\lceil (c-2)l_0/2 \rceil}\right) + \Theta\left(n^{\frac{3}{2}} e^{n\omega_{q,c,d}((l_0+4)/n)}\right)\\
&\qquad + \Theta\left(n^{\frac{3}{2}} e^{n\omega_{q,c,d}(\alpha)}\right)\\
&\quad \overset{\text{(d)}}{\le} \Theta\left(n^{-\lceil (c-2)l_0/2 \rceil}\right) + \Theta\left(n^{\frac{3}{2}} n^{-(c-2)(l_0+4)/2}\right)\\
&\qquad + \Theta\left(n^{\frac{3}{2}} e^{n\omega_{q,c,d}(\alpha)}\right)\\
&\quad \overset{\text{(e)}}{\le} \Theta\left(n^{-\lceil (c-2)l_0/2 \rceil}\right) + \Theta\left(n^{\frac{3}{2}} e^{n\omega_{q,c,d}(\alpha)}\right)
\end{aligned}$$

where (a) follows from Markov's inequality, (b) from Theorems 3.6 and 3.11, Lemma A.1, and the inequality $l(n-l) \le n^2/4$, (c) from Theorem 5.6, which shows that $\omega_{q,c,d}(x)$ with $x \in [(l_0+4)/n, \alpha]$ is upper bounded by either $\omega_{q,c,d}((l_0+4)/n)$ or $\omega_{q,c,d}(\alpha)$, (d) from Theorem 6.1, and (e) follows from $c \ge 3$.

The above inequality holds in all cases. When $q = 2$ and cl_0 is odd, Theorem 3.11 shows that $E[A_{q,c,d}^{(n)}(l_0)] = 0$, so we can further improve this inequality by simply replacing l_0 with $l_0 + 1$. The proof is complete. □

Remark 6.3: If taking $l_0 = 1$ in Theorem 6.2, we have

$$P\Big\{\mathrm{d}_{\min}(\mathcal{C}_{q,c,d}^{(n)}) \le n\alpha\Big\} \le \Theta\left(n^{-\lceil (c-2)/2\rceil}\right) + \Theta\left(n^{\frac{3}{2}} e^{n\omega_{q,c,d}(\alpha)}\right).^2 \tag{50}$$

Recall that $\omega_{q,c,d}(x)$ has a unique zero $x_0(q,c,d)$ in $(0, 1 - 1/q)$, so we have

$$P\Big\{\mathrm{d}_{\min}(\mathcal{C}_{q,c,d}^{(n)}) \le n\alpha\Big\} \le \Theta\left(n^{-\lceil (c-2)/2\rceil}\right) \tag{51}$$

for any $\alpha \in (0, x_0(q,c,d))$. Moreover, when $c \ge 5$, it follows from the Borel-Cantelli lemma that for any $\epsilon > 0$, the probability of the event

$$\left\{\frac{1}{n}\,\mathrm{d}_{\min}(\mathcal{C}_{q,c,d}^{(n)}) \le x_0(q,c,d) - \epsilon \text{ for infinitely many } n\right\}$$

is zero, so that

$$P\Big\{\liminf_{n\to\infty} \frac{1}{n}\,\mathrm{d}_{\min}(\mathcal{C}_{q,c,d}^{(n)}) \ge x_0(q,c,d)\Big\} = 1. \tag{52}$$

The formula (50), for $q = 2$, was first proved (in a slightly stronger form for a different ensemble) by Gallager in [1]. As for the general case of $q > 2$, Bennatan and Burshtein first showed in [8] that there exists some $\gamma > 0$ such that

$$P\Big\{\mathrm{d}_{\min}(\mathcal{C}_{q,c,d}^{(n)}) \le n\gamma\Big\} \le \Theta\left(n^{1-c/2}\right)$$

which is clearly weaker than (51). In [9], Como and Fagnani proved a result similar to (51).

Compared with previous results, the advantage of Theorem 6.2 is that we can use it to obtain results much better than (50) by removing bad codes from the original ensemble. This viewpoint is formulated in the following theorem, which is an easy consequence of Theorem 6.2.

Theorem 6.4: Let $q \ge 2$, $d \ge c \ge 3$, $l_0 \ge 2$, and $\alpha \in (0, 1 - 1/q)$. Let $\Phi_n : \{\text{All subspaces of } \mathbb{F}_q^n\} \to \{0, 1\}$ be a test function of linear codes such that for every linear code C, $\Phi_n(C) = 1$ implies $\mathrm{d}_{\min}(C) \ge l_0$. If $E[\Phi_n(\mathcal{C}_{q,c,d}^{(n)})] \ge \Theta(\phi(n))$ for some map $\phi(n) : \mathbb{N} \to [0, 1]$, then

$$P\Big\{\mathrm{d}_{\min}(\mathcal{C}_{q,c,d}^{(n)}) \le n\alpha \Big| \, \Phi_n(\mathcal{C}_{q,c,d}^{(n)}) = 1\Big\} \le \Theta\left(\frac{n^{-\lceil (c-2)(l_0+\Delta)/2\rceil}}{\phi(n)}\right) + \Theta\left(\frac{n^{\frac{3}{2}} e^{n\omega_{q,c,d}(\alpha)}}{\phi(n)}\right) \tag{53}$$

where Δ is defined by (49).

The proof is left to the reader.

Remark 6.5: A simple test function can be defined by checking whether the parity-check matrix of a linear code contains all-zero columns. Then $\Phi_n(C) = 1$ if and only if the parity-check matrix of C contains no all-zero columns. It is clear that $\Phi_n(C) = 1$ is equivalent to $\mathrm{d}_{\min}(C) \ge 2$, so it follows from (51) that

$$E\Big[\Phi_n(\mathcal{C}_{q,c,d}^{(n)})\Big] = P\Big\{\mathrm{d}_{\min}(\mathcal{C}_{q,c,d}^{(n)}) \ge 2\Big\} = \Theta(1).$$

Consequently, we have

$$P\Big\{\mathrm{d}_{\min}(\mathcal{C}_{q,c,d}^{(n)}) \le n\alpha \Big| \, \Phi_n(\mathcal{C}_{q,c,d}^{(n)}) = 1\Big\} \le \Theta\left(n^{2-c}\right) + \Theta\left(n^{\frac{3}{2}} e^{n\omega_{q,c,d}(\alpha)}\right). \tag{54}$$

VII. Conclusion

We provided a thorough analysis of the average weight distributions of regular LDPC code ensembles over finite fields. The primary results are Theorems 3.11, 4.5, 5.6, and 6.1, which are important for any analysis of regular LDPC codes based on the weight distribution. Furthermore, we proved a general result (Theorem 6.2) on the minimum distance of individual codes in a regular LDPC code ensemble, which includes all previous results as special cases.

Acknowledgment

The authors would like to thank the anonymous reviewers for their helpful comments.

Appendix A
Some Useful Inequalities

Lemma A.1: For any $n \in \mathbb{N}$, define the function

$$\beta_n(l) \triangleq H_2\left(\frac{l}{n}\right) - \frac{1}{n}\ln\binom{n}{l} \qquad \forall l = 0, 1, \ldots, n.$$

Then

$$0 \le \beta_n(l) \le \frac{1}{2n}\ln\left(\frac{l(n-l)}{n}\right) + \Theta(n^{-1}) \qquad \forall 0 < l < n$$

and $\beta_n(0) = \beta_n(n) = 0$.

Sketch of Proof: Using Stirling's approximation:

$$n! = \sqrt{2\pi n}\left(\frac{n}{e}\right)^n e^{\lambda_n} \qquad \forall n \ge 1$$

where $1/(12n+1) < \lambda_n < 1/(12n)$. □

Lemma A.2: For all $x \in [0, 1]$ and $d \in \mathbb{N}$,

$$(1-x)^d \le 1 - dx + \frac{d(d-1)}{2}x^2.$$

Proof: The inequality holds trivially for $d = 1$. Now suppose $d \ge 2$, then by Taylor's theorem, it follows that

$$(1-x)^d = 1 - dx + \frac{d(d-1)(1-y)^{d-2}}{2}x^2$$

for some $y \in [0, x]$. This thus concludes the proposition. □

[2] When $q = 2$ and c is odd, we have a tighter upper bound $\Theta(n^{2-c}) + \Theta(n^{\frac{3}{2}} e^{n\omega_{2,c,d}(\alpha)})$. But for simplicity, we ignore this special case.

Appendix B
Derivatives of $H_q(x)$, $D(x\|\hat{x})$, and $\rho_{q,d}(x)$

Lemma B.1:

$$\begin{aligned}
\frac{dH_q(x)}{dx} &= \ln\frac{1-x}{x} + \ln(q-1)\\
\frac{\partial D(x\|\hat{x})}{\partial x} &= \ln\frac{x(1-\hat{x})}{\hat{x}(1-x)}\\
\frac{\partial D(x\|\hat{x})}{\partial \hat{x}} &= \frac{\hat{x}-x}{\hat{x}(1-\hat{x})}\\
\frac{d\rho_{q,d}(x)}{dx} &= -\frac{qd\left(1-\dfrac{qx}{q-1}\right)^{d-1}}{1+(q-1)\left(1-\dfrac{qx}{q-1}\right)^{d}}.
\end{aligned}$$

where $\rho_{q,d}(x)$ is defined by (8).

The proof is left to the reader.

Appendix C
Descartes' Rule of Signs

Theorem C.1 (Descartes' Rule of Signs): If the terms of a univariate polynomial with real coefficients are ordered by ascending or descending variable exponent, then the number of positive roots of the polynomial (counted with their multiplicities) is either equal to the number of sign changes between consecutive nonzero coefficients, or less than it by a multiple of 2. Since the negative roots of the polynomial equation $f(x) = 0$ are positive roots of the equation $f(-x) = 0$, the rule can be readily applied to help count the negative roots as well.

For a proof we refer the reader to [15].

Appendix D
Proofs of Lemmas in Section IV

Proof of Lemma 4.1: By definition (7), (18) follows immediately. Using Lemma B.1 and the change of variables (16) yields

$$\begin{aligned}
\frac{\partial\delta_{q,d}(x,\hat{x})}{\partial\hat{x}} &= \frac{qd(z-\hat{z})}{(1-\hat{z})[1+(q-1)\hat{z}]} - \frac{qd\hat{z}^{d-1}}{1+(q-1)\hat{z}^d}\\
&= \frac{qd\{z-\hat{z}-\hat{z}^{d-1}-[(q-2)-(q-1)z]\hat{z}^d\}}{(1-\hat{z})[1+(q-1)\hat{z}][1+(q-1)\hat{z}^d]}\\
&= -\frac{qd(\zeta_{q,d}(\hat{z})-z)}{(1-\hat{z})[1+(q-1)\hat{z}]}
\end{aligned}$$

as desired. □

Proof of Lemma 4.2: To prove the lemma, we have to show that the derivative of $\zeta_{q,d}(\hat{z})$ is continuous on $[-1/(q-1), 1]$ and positive on $(-1/(q-1), 1)$. Some tedious manipulation yields

$$\zeta'_{q,d}(\hat{z}) = \frac{f(\hat{z})}{[1+(q-1)\hat{z}^d]^2}$$

where

$$\begin{aligned}
f(\hat{z}) \triangleq 1 &+ (d-1)\hat{z}^{d-2} + (q-2)d\hat{z}^{d-1} - (q-1)(d-1)\hat{z}^d\\
&- (q-1)\hat{z}^{2d-2}.
\end{aligned}$$

The continuity is obvious, even if $q = 2$ and d is odd. Our task is now to show that $f(\hat{z})$ is positive on $(-1/(q-1), 1)$. The proof consists of two parts.

First, we show that $f(\hat{z})$ is positive on $[0, 1)$. Note that the coefficients of $f(\hat{z})$ have signs $+, +, +, -, -$. By Theorem C.1 it follows that $f(\hat{z})$ has a unique positive zero. Since $f(0) = 1 > 0$ and $f(1) = 0$, it is clear that $f(\hat{z}) > 0$ for all $\hat{z} \in [0, 1)$.

Second, we show that $f(\hat{z})$ is also positive on $(-1/(q-1), 0)$ for both odd and even d.

For odd d we have

$$\begin{aligned}
f(-\hat{z}) = 1 &- (d-1)\hat{z}^{d-2} + (q-2)d\hat{z}^{d-1}\\
&+ (q-1)(d-1)\hat{z}^d - (q-1)\hat{z}^{2d-2}.
\end{aligned}$$

If $q \geq 3$ then for all $\hat{z} \in (0, 1/(q-1))$,

$$\begin{aligned}
f(-\hat{z}) &> 1 - (d-1)\hat{z}^{d-2}\\
&> 1 - \frac{(d-1)}{(q-1)^{d-2}}\\
&\geq \frac{2^{d-1}-(d-1)}{(q-1)^{d-2}}\\
&\geq 0.
\end{aligned}$$

As for the case of $q = 2$, $f(-\hat{z})$ reduces to

$$1 - (d-1)\hat{z}^{d-2} + (d-1)\hat{z}^d - \hat{z}^{2d-2}$$

which can be factorized as

$$(1-\hat{z})^3\left[\sum_{i=0}^{d-3}\frac{(i+1)(i+2)}{2}\left(\hat{z}^i + \hat{z}^{2d-5-i}\right)\right] \tag{55}$$

so that $f(-\hat{z}) > 0$ for all $\hat{z} \in (0, 1)$.

For even d we have

$$\begin{aligned}
f(-\hat{z}) &= 1 + (d-1)\hat{z}^{d-2} - (q-2)d\hat{z}^{d-1}\\
&\quad - (q-1)(d-1)\hat{z}^d - (q-1)\hat{z}^{2d-2}\\
&> \hat{z}^{d-2} + (d-1)\hat{z}^{d-2} - \frac{(q-2)d}{q-1}\hat{z}^{d-2}\\
&\quad - \frac{d-1}{q-1}\hat{z}^{d-2} - \frac{1}{q-1}\hat{z}^{d-2}\\
&= 0
\end{aligned}$$

for all $\hat{z} \in (0, 1/(q-1))$. The proof is complete. □

Sketch of Proof of Lemma 4.3: Identity (21) is proved by a straightforward argument using definition (20). Equations (22b), (23), and (24) are immediate consequence of (21). As for (22a), we note that (21) with $q = 2$ and odd d gives

$$\zeta_{2,d}(-1) + 1 = \left.\frac{z^{d-1}(1-z)}{1-z+z^2-\cdots+z^{d-1}}\right|_{z=-1} = \frac{2}{d}$$

so that $\zeta_{2,d}(-1) = 2/d - 1$. □

Proof of Lemma 4.4: Lemmas 4.2 and 4.3 show that the range of $\zeta_{q,d}(\hat{z})$ for $\hat{z} \in [-1/(q-1), 1]$ is

$$\left[\zeta_{q,d}\left(-\frac{1}{q-1}\right), \zeta_{q,d}(1)\right] = [z_1, 1]$$

and therefore the equation $\zeta_{2,d}(\hat{z}) - z = 0$ has a unique solution in $[-1/(q-1), 1]$ for each $z \in [z_1, 1]$ and has no solution in $[-1/(q-1), 1]$ for $z < z_1$.

Since $\zeta_{q,d}(\hat{z})$ is continuously differentiable on $[-1/(q-1),1]$ and its derivative is positive on $(-1/(q-1),1)$, it follows from the inverse function theorem that the solution $\hat{z}_1(z)$ is continuously differentiable on $(z_1,1)$ and its derivative is also positive on $(z_1,1)$. The continuity of $\hat{z}_1(z)$ at endpoints also follows. Moreover, Lemma 4.3 shows that

$$\begin{array}{ll}
\zeta_{q,d}(z)=z_1 & \text{if } z=-\frac{1}{q-1}\\
\zeta_{q,d}(z)>z & \text{if } z\in(-\frac{1}{q-1},0) \text{ and } d \text{ is odd}\\
\zeta_{q,d}(z)<z & \text{if } z\in(-\frac{1}{q-1},0) \text{ and } d \text{ is even}\\
\zeta_{q,d}(z)=0 & \text{if } z=0\\
\zeta_{q,d}(z)>z & \text{if } z\in(0,1)\\
\zeta_{q,d}(z)=1 & \text{if } z=1.
\end{array}$$

This implies that $\hat{z}_1(z)\in I'_{q,d}(z)$. □

APPENDIX E
PROOFS OF LEMMAS IN SECTION V

Proof of Lemma 5.2: Definition (5) and equation (29) show that

$$\begin{aligned}
\frac{d\omega_{q,c,d}(x)}{dx} &= \frac{dH_q(x)}{dx}+c\ln\frac{x(1-\hat{x}_1)}{\hat{x}_1(1-x)}\\
&\overset{(a)}{=} \ln\frac{1-x}{x}+\ln(q-1)+c\ln\frac{x(1-\hat{x}_1)}{\hat{x}_1(1-x)}\\
&= \ln\left[\left(\frac{x}{1-x}\right)^{c-1}\left(\frac{1-\hat{x}_1}{\hat{x}_1}\right)^{c}\right]+\ln(q-1)
\end{aligned}$$

where (a) follows from Lemma B.1. By Lemma 4.1, equation (28) is equivalent to $\zeta_{q,d}(\hat{z}_1)-z=0$, where $z=1-qx/(q-1)$ and $\hat{z}_1=1-q\hat{x}_1/(q-1)$. After some manipulations, we obtain

$$\frac{x}{\hat{x}_1}=\frac{1-z}{1-\hat{z}_1}=\frac{1-\hat{z}_1^{d-1}}{1+(q-1)\hat{z}_1^{d}}$$

and

$$\frac{1-x}{1-\hat{x}_1}=\frac{1+(q-1)z}{1+(q-1)\hat{z}_1}=\frac{1+(q-1)\hat{z}_1^{d-1}}{1+(q-1)\hat{z}_1^{d}}.$$

Then

$$\begin{aligned}
\frac{d\omega_{q,c,d}(x)}{dx} &= \ln\left\{\frac{(q-1)(1-\hat{x}_1)}{\hat{x}_1}\left[\frac{x(1-\hat{x}_1)}{\hat{x}_1(1-x)}\right]^{c-1}\right\}\\
&= \ln\left\{\frac{1+(q-1)\hat{z}_1}{1-\hat{z}_1}\left[\frac{1-\hat{z}_1^{d-1}}{1+(q-1)\hat{z}_1^{d-1}}\right]^{c-1}\right\}.
\end{aligned}$$

The proof is complete. □

Proof of Lemma 5.3: From Theorem 4.5, it follows that $\lim_{x\to 0^+}\hat{z}_1=1$. Then equation (36) with $c=1$ and $c\geq 3$ gives (37a) and (37c), respectively. As for $c=2$, we have

$$\begin{aligned}
&\lim_{x\to 0^+}\frac{d\omega_{q,c,d}(x)}{dx}\\
&=\lim_{\hat{z}_1\to 1^-}\ln\left\{\frac{[1+(q-1)\hat{z}_1](1-\hat{z}_1^{d-1})}{(1-\hat{z}_1)[1+(q-1)\hat{z}_1^{d-1}]}\right\}\\
&=\lim_{\hat{z}_1\to 1^-}\ln\left\{\frac{[1+(q-1)\hat{z}_1](1+\hat{z}_1+\cdots+\hat{z}_1^{d-2})}{1+(q-1)\hat{z}_1^{d-1}}\right\}\\
&=\ln(d-1).
\end{aligned}$$

By the symmetric property (Remark 3.10), we also obtain (39).

From Theorem 4.5, it follows that

$$\hat{z}_1\left(1-\frac{1}{q}\right)=1-\frac{q(1-1/q)}{q-1}=0.$$

This together with equation (36) gives (38).

Again by Theorem 4.5, it follows that $\lim_{x\to x_1^-}\hat{z}_1=-1/(q-1)$. Then (36) with $q\neq 2$ or d odd gives (40). □

Proof of Lemma 5.4: It follows from Lemma 5.2 that

$$\begin{aligned}
&\frac{d}{d\hat{z}_1}\left(\frac{d\omega_{q,c,d}(x)}{dx}\right)\\
&=\frac{q}{[1+(q-1)\hat{z}_1](1-\hat{z}_1)}-\frac{q(c-1)(d-1)\hat{z}_1^{d-2}}{(1-\hat{z}_1^{d-1})[1+(q-1)\hat{z}_1^{d-1}]}\\
&=\frac{q\xi_{q,c,d}(\hat{z})}{(1-\hat{z}_1^{d-1})[1+(q-1)\hat{z}_1][1+(q-1)\hat{z}_1^{d-1}]}.
\end{aligned}$$

This concludes (42), while the first equality with $c=1$ gives (44). □

Proof of Lemma 5.5: Since $\xi_{q,c,d}(0)=1$, it suffices to determine all zeros of $\xi_{q,c,d}(\hat{z})$ in $(-1/(q-1),1)$. The proof consists of two parts.

First, we check the zeros of $\xi_{q,c,d}(\hat{z})$ in $(0,1)$. We note that the coefficients of $\xi_{q,c,d}(\hat{z})$ have signs $+,\ldots,+,-,-,+,\ldots,+$. By Theorem C.1 it follows that $\xi_{q,c,d}(\hat{z})$ has zero or two positive zeros. On the other hand,

$$\xi_{q,c,d}(0)=1,\ \xi_{q,c,d}(1)=-q(c-2)(d-1),\ \xi_{q,c,d}(\infty)=\infty$$

and

$$\xi'_{q,2,d}(1)=\frac{1}{2}(q-2)(d-1)(d-2).$$

Then for $q\geq 2$ and $d\geq c\geq 3$, $\xi_{q,c,d}(\hat{z})$ has a unique zero $\hat{z}_2$ in $(0,1)$. As for $c=2$, $\xi_{q,2,d}(\hat{z})$ with $q\geq 3$ has a unique zero $\hat{z}_2$ in $(0,1)$ since $\xi_{q,2,d}(1)=0$ and $\xi'_{q,2,d}(1)>0$, while $\xi_{2,2,d}(\hat{z})$ has only one zero $\hat{z}=1$ in $(0,\infty)$ since $\xi'_{2,2,d}(1)=0$ (a zero of multiplicity 2), so that $\xi_{2,2,d}(\hat{z})$ is positive on $(0,1)$.

Second, we check the zeros of $\xi_{q,c,d}(\hat{z})$ in $(-1/(q-1),1)$. To facilitate the analysis, we consider the function

$$f_{q,c,d}(\hat{z})\triangleq(1+\hat{z})\xi_{q,c,d}(-\hat{z}).$$

Then the zeros of $\xi_{q,c,d}(\hat{z})$ in $(-1/(q-1),0)$ are just the zeros of $f_{q,c,d}(\hat{z})$ in $(0,1/(q-1))$.

If d is odd, we have

$$\begin{aligned}
f_{q,c,d}(\hat{z})&=(1-\hat{z}^{d-1})[1+(q-1)\hat{z}^{d-1}]\\
&\quad+(c-1)(d-1)\hat{z}^{d-2}(1+\hat{z})[1-(q-1)\hat{z}]
\end{aligned}$$

which is clearly positive for all $\hat{z}\in(0,1/(q-1))$.

If d is even, we have

$$\begin{aligned}
f_{q,c,d}(\hat{z})&=(1+\hat{z}^{d-1})[1-(q-1)\hat{z}^{d-1}]\\
&\quad-(c-1)(d-1)\hat{z}^{d-2}(1+\hat{z})[1-(q-1)\hat{z}]\\
&=1-(c-1)(d-1)\hat{z}^{d-2}\\
&\quad+(q-2)[(c-1)(d-1)-1]\hat{z}^{d-1}\\
&\quad+(q-1)(c-1)(d-1)\hat{z}^{d}-(q-1)\hat{z}^{2d-2}.
\end{aligned}$$

When $q=2$, it reduces to

$$f_{2,c,d}(\hat{z})=1-(c-1)(d-1)\hat{z}^{d-2}+(c-1)(d-1)\hat{z}^{d}-\hat{z}^{2d-2}.$$

Since the coefficients of $f_{2,c,d}(\hat{z})$ have signs $+,-,+,-$, it follows from Theorem C.1 that $f_{2,c,d}(\hat{z})$ has one or three positive zeros. Moreover, we note that

$$f_{2,c,d}(0) = 1,\ f_{2,c,d}(1) = 0,\ f_{2,c,d}(\infty) = -\infty$$

and

$$f'_{2,c,d}(1) = 2(c-2)(d-1).$$

Then $f_{2,c,d}(\hat{z})$ with $c \geq 3$ has a unique zero $\hat{z}'_2$ in $(0,1)$, while $f_{2,2,d}(\hat{z})$ is positive on $(0,1)$ because of (55). Finally, let us show that $f_{q,c,d}(\hat{z})$ is positive on $(0, 1/(q-1))$ for $q \geq 3$, $c \geq 2$, and $d \geq \max\{c, 4\}$. Since $q \geq 3$, $c \geq 2$, $d \geq 4$, and $\hat{z} < 1/(q-1)$,

$$\begin{aligned} f_{q,c,d}(\hat{z}) &> 1-(c-1)(d-1)\hat{z}^{d-2}(1-\hat{z}-2\hat{z}^2) \\ &\qquad - \hat{z}^{d-1} - \hat{z}^{2d-3} && (56) \\ &> 1-(c-1)(d-1)\hat{z}^{d-2}. && (57) \end{aligned}$$

For $\hat{z} \in (0, \frac{1}{3}]$, inequality (57) shows that

$$f_{q,c,d}(\hat{z}) > 1-(d-1)^2\left(\frac{1}{3}\right)^{d-2} \geq 1-(4-1)^2\left(\frac{1}{3}\right)^{4-2} = 0.$$

For $\hat{z} \in (\frac{1}{3}, \frac{2}{5}]$, inequality (56) shows that

$$\begin{aligned} f_{q,c,d}(\hat{z}) &> 1 - \frac{4(d-1)^2}{9}\left(\frac{2}{5}\right)^{d-2} - \left(\frac{2}{5}\right)^{d-1} - \left(\frac{2}{5}\right)^{2d-3} \\ &\geq 1 - \frac{4}{9}\cdot 3^2\left(\frac{2}{5}\right)^2 - \left(\frac{2}{5}\right)^3 - \left(\frac{2}{5}\right)^5 \\ &= \frac{893}{3125}. \end{aligned}$$

For $\hat{z} \in (\frac{2}{5}, \frac{1}{2})$, inequality (56) shows that

$$\begin{aligned} f_{q,c,d}(\hat{z}) &> 1 - \frac{7(d-1)^2}{25}\left(\frac{1}{2}\right)^{d-2} - \left(\frac{1}{2}\right)^{d-1} - \left(\frac{1}{2}\right)^{2d-3} \\ &\geq 1 - \frac{7}{25}\cdot 3^2\left(\frac{1}{2}\right)^2 - \left(\frac{1}{2}\right)^3 - \left(\frac{1}{2}\right)^5 \\ &= \frac{171}{800}. \end{aligned}$$

The proof is complete. □

References

[1] R. G. Gallager, *Low-Density Parity-Check Codes*. Cambridge, MA: MIT Press, 1963.

[2] S. Litsyn and V. Shevelev, "On ensembles of low-density parity-check codes: Asymptotic distance distributions," *IEEE Trans. Inf. Theory*, vol. 48, no. 4, pp. 887–908, Apr. 2002.

[3] ——, "Distance distributions in ensembles of irregular low-density parity-check codes," *IEEE Trans. Inf. Theory*, vol. 49, no. 12, pp. 3140–3159, Dec. 2003.

[4] D. Burshtein and G. Miller, "Asymptotic enumeration methods for analyzing LDPC codes," *IEEE Trans. Inf. Theory*, vol. 50, no. 6, pp. 1115–1131, Jun. 2004.

[5] C. Di, T. J. Richardson, and R. L. Urbanke, "Weight distribution of low-density parity-check codes," *IEEE Trans. Inf. Theory*, vol. 52, no. 11, pp. 4839–4855, Nov. 2006.

[6] V. Rathi, "On the asymptotic weight and stopping set distribution of regular LDPC ensembles," *IEEE Trans. Inf. Theory*, vol. 52, no. 9, pp. 4212–4218, Sep. 2006.

[7] M. F. Flanagan, E. Paolini, M. Chiani, and M. P. C. Fossorier, "Growth rate of the weight distribution of doubly-generalized LDPC codes: General case and efficient evaluation," in *Proc. IEEE Global Communications Conf.*, Honolulu, HI, Nov. 2009, pp. 926–931.

[8] A. Bennatan and D. Burshtein, "On the application of LDPC codes to arbitrary discrete-memoryless channels," *IEEE Trans. Inf. Theory*, vol. 50, no. 3, pp. 417–437, Mar. 2004.

[9] G. Como and F. Fagnani, "Average spectra and minimum distances of low-density parity-check codes over abelian groups," *SIAM J. Discrete Math.*, vol. 23, no. 1, pp. 19–53, 2008.

[10] I. Andriyanova, V. Rathi, and J.-P. Tillich, "Binary weight distribution of non-binary LDPC codes," in *Proc. IEEE Int. Symp. Information Theory*, Coex, Seoul, Korea, Jun. 2009, pp. 65–69.

[11] S. Yang, T. Honold, Y. Chen, Z. Zhang, and P. Qiu, "Constructing linear codes with good spectra," *IEEE Trans. Inf. Theory*, 2009, submitted for publication.

[12] M. G. Luby, M. Mitzenmacher, M. A. Shokrollahi, and D. A. Spielman, "Improved low-density parity-check codes using irregular graphs," *IEEE Trans. Inf. Theory*, vol. 47, no. 2, pp. 585–598, Feb. 2001.

[13] T. J. Richardson and R. L. Urbanke, "The capacity of low-density parity-check codes under message-passing decoding," *IEEE Trans. Inf. Theory*, vol. 47, no. 2, pp. 599–618, Feb. 2001.

[14] W. C. Huffman and V. Pless, *Fundamentals of Error-Correcting Codes*. New York: Cambridge University Press, 2003.

[15] X. Wang, "A simple proof of Descartes's rule of signs," *The American Mathematical Monthly*, vol. 111, no. 6, pp. 525–526, Jun. 2004.

Shengtian Yang (S'05–M'06) was born in Hangzhou, Zhejiang, China, in 1976. He received the B.S. and M.S. degrees in biomedical engineering, and the Ph.D. degree in electrical engineering from Zhejiang University, Hangzhou, China in 1999, 2002, and 2005, respectively.

From June 2005 to December 2007, he was a Postdoctoral Fellow at the Department of Information Science and Electronic Engineering, Zhejiang University. From December 2007 to January 2010, he was an Associate Professor at the Department of Information Science and Electronic Engineering, Zhejiang University. Currently, he is a self-employed Independent Researcher in Hangzhou, China. His research interests include information theory, coding theory, and design and analysis of algorithms.

Thomas Honold (M'95) was born in Munich, Germany, in 1962. He received his Diplom (1990), doctoral degree (1994) and Habilitation (2000, the qualification for university teaching in Germany) in Mathematics from TU Munich, Germany. He has held appointments at TU Munich, University of Eichstätt, Germany, and the German Institute of Science and Technology, Singapore. Since 2007 he is working as Associate Professor for the Department of Information Science and Electronic Engineering, Zhejiang University, Hangzhou. His main research interest is coding theory and geometry over finite fields and rings.

Yan Chen (S'06–M'10) was born in Hangzhou, Zhejiang, China, in 1982. She received the B.Sc. and the Ph. D degree in information and communication engineering from Zhejiang University, Hangzhou, China, in 2004 and 2009, respectively. She has been a Visiting Researcher at the Department of Electronic and Computer Engineering, Hong Kong University of Science and Technology, Hong Kong. After graduation, she joined Huawei Technologies (Shanghai) Co., Ltd. and is currently working as a Research Engineer in the Central Research Department. Her current research interests include green network information theory, energy-efficient network architecture and management, fundamental tradeoffs on green wireless network design, as well as the radio technologies and resource allocation optimization algorithms therein.

Zhaoyang Zhang (M'02) was born in Huanggang, Hubei, China, in 1973. He received the B.Sc. degree in radio technology and the Ph.D degree in information and communication engineering from Zhejiang University, Hangzhou, China, in 1994 and 1998, respectively.

Since 1998, he has been with the Department of Information Science and Electronic Engineering, Zhejiang University, Hangzhou, China, where he is currently a Professor. His current research interests include information theory and signal processing theory with emphsis on their applications in wireless communications and networks.

Peiliang Qiu (M'03) was born in Shanghai, China, in 1944. He received the B.S. degree from the Harbin Institute of Technology, Harbin, China, in 1967 and the M.S. degree from the Graduate School of Chinese Academy of Science, Beijing, in 1981, both in electronics engineering.

From 1968 to 1978, he was a Research Engineer at Jiangnan Electronic Technology Institute. Since November 1981, he has been with Zhejiang University, Hangzhou, China, where he is currently a Professor at the Department of Information Science and Electronic Engineering. His current research interests include digital communications, information theory, and wireless networks.